UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/687,320	10/16/2003	Frank J. Hammond II	413130	8493

30955 7590 12/24/2009

LATHROP & GAGE LLP
4845 PEARL EAST CIRCLE
SUITE 201
BOULDER, CO 80301

EXAMINER	
CERVETTI, DAVID GARCIA	
ART UNIT	**PAPER NUMBER**
2436	

NOTIFICATION DATE	DELIVERY MODE
12/24/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patent@lathropgage.com

Office Action Summary	Application No.	Applicant(s)	
	10/687,320	HAMMOND ET AL.	
	Examiner	Art Unit	
	David García Cervetti	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 September 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-15* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *26 September 2007* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's arguments filed 9/21/2009 have been fully considered.

2. Claims 1-15 are pending and have been examined.

Response to Amendment

3. The rejection under 35 USC 101 is withdrawn.

4. **Examiner's Note:** Examiner has cited particular columns and line numbers in the references as applied to the claims below for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested that the applicant, in preparing the responses, fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

5. Regarding the arguments against Vallee, Examiner respectfully points out that Vallee teaches the use of a confidence authority (trusted source) and the Fiat-Shamir and Gillou-Quisquater protocols teach the use of "large prime numbers" (see NPL "How to prove yourself: practical solutions to identification and signature problems" by Amos Fiat and Adi Shamir – 1987, sec.2.2, page 187) and to par.177 of Vallee where it teaches access to a server (secure area of a host). It is further noted that the claim itself does not expressly claim "stored in a secure area" as argued. Applicant's arguments are not persuasive.

6. While the breadth of the claims in the application should always be carefully noted; that is, the examiner should be fully aware of what the claims do not call for, as well as what they do require; during patent examination, the claims are given the broadest reasonable interpretation consistent with the specification.

7. The basis for the admission is found on par.3 (Background, not summary), the use of Fiat Shamir is found on Vallee. While Bartram uses one particular protocol, the architecture is provided, replacing one protocol with another falls within what someone of ordinary skill in the art would have found to be obvious. Arguments are not persuasive.

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Liskov et al. (6411715).

Claim Rejections - 35 USC § 112

9. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

10. Claims 1-15 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

11. The term "large prime numbers" in the claims is a relative term which renders the claim indefinite. The term is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention.

Claim Rejections - 35 USC § 102

12. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

13. Claims 5-6 are rejected under 35 U.S.C. 102(e) as being anticipated by Vallee et al. (US 2004/0177252, hereinafter Vallee).

Regarding claim 5, Vallee teaches

a method of protecting a host computer from unauthorized access by a client computer over a computer network, comprising the steps of (abstract, authentication):

installing a prover agent application on the client computer (par.7-12, entity to be authenticated);

installing a verifier agent application on the host computer (par.7-12, authenticator);

creating a trusted source application on the computer network to generate and publish encrypted values of a secret and product of first and second large prime numbers; reading the encrypted values for the secret and product, by the prover and verifier from the trusted source; decrypting the secret, by the prover and verifier; decrypting the product, by the prover and verifier; and performing a plurality of verification dialog between the prover and verifier over the network, wherein the prover demonstrates knowledge of the secret and product without exposing the values of the secret and product, and wherein the client is denied access to a secure area of the host when the prover fails to demonstrate knowledge of the secret and product and granted

access to the secure area when the client succeeds in demonstrating knowledge of the secret and product (par.90-108, Fiat-Shamir protocol).

Regarding claim 6, Vallee teaches wherein the steps of decrypting the secret and product further utilize previous values of the secret and product as operators in the modulus inverse operations, to decrypt new values for the secret and the product (par.90-108, Fiat-Shamir protocol).

Claim Rejections - 35 USC § 103

14. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

15. Claims 1, 3, 8, and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bartram et al. (US 2004/0054885, hereinafter Bartram), and further in view of Admission (specification, pages 1-3, USE of zero knowledge protocols).

Regarding claims 1, 8, and 13, Bartram teaches

a method of non-centralized authentication for a computer network, comprising steps of (abstract, peer-to-peer):

establishing a first computer having a first authentication agent and a first prover agent on the computer network (par.26-29, authentication software);

detecting a first authentication request over the computer network from a second computer having a second prover agent (par.26-29, authenticate another unit);

authenticating the second prover agent through a identification protocol (par.26-29, authenticate another unit); and

promoting the second computer with a second authentication agent to perform authentication for the computer network (par.31-32, second unit authenticates third unit for first unit).

Bartram does not expressly disclose that the authentication/ identification protocol is a zero-knowledge protocol.

However, Applicant admits that the **use** of zero knowledge protocols was conventional and well known at the time the invention was made. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to **use** zero knowledge authentication protocols with the invention of Bartram since it would extend authentication capabilities to other devices and other protocols.

Regarding claim 3, the combination of Bartram and Admission teaches detecting a second authentication request over the computer network from a third computer having a third prover agent (par.26-29); authenticating the third prover agent through a zero-knowledge identification protocol with the second authentication agent (par.31-32); and promoting the third computer with a third authentication agent to perform authentication for the computer network (par.31-32).

16. Claims 2, 4, and 9-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bartram and Admission, and further in view of Vallee.

Regarding claims 2 and 9, the combination of Bartram and Admission does not expressly disclose, however, Vallee teaches periodically generating and distributing a new secret to the first and second authentication agents (par.90-108, Fiat-Shamir protocol). Therefore, it would have been obvious to one having ordinary skill in the art at

the time the invention was made to publish new secrets as taught by Fiat-Shamir with the invention of Bartram. One of ordinary skill in the art would have been motivated to perform such a modification to renew the secret information.

Regarding claim 4, the combination of Bartram and Admission does not expressly disclose, however, Vallee teaches periodically publishing encrypted numbers for the zero-knowledge identification protocol, including the steps of:

generating first and second large prime numbers; calculating a product of the first and second large prime numbers; generating a secret to have a value relatively prime to the product, greater than zero and less than the product; encrypting the product; encrypting the secret; and publishing encrypted values of the secret and product (par.90-108, Fiat-Shamir protocol). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to publish new secrets as taught by Fiat-Shamir with the invention of Bartram. One of ordinary skill in the art would have been motivated to perform such a modification to renew the secret information.

Regarding claim 10, the combination of Bartram and Admission teaches the requesting computer comprising a cell phone (par.2-3).

Regarding claim 11, the combination of Bartram and Admission teaches the computer network comprising one or more of the Internet, a local area network, a communications link, and a wireless network (par.2-3).

Regarding claim 12, the combination of Bartram and Admission teaches the authentication agents and prover agents being installed on each of the computers through common software (par.25-34).

Allowable Subject Matter

17. Claims 7 and 14 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims. Claim 15 would be allowable.

Conclusion

18. Any inquiry concerning this communication or earlier communications from the examiner should be directed to DAVID CERVETTI whose telephone number is (571)272-5861. The examiner can normally be reached on Monday-Tuesday and Thursday-Friday.
19. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on (571)272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.
20. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/David García Cervetti/
Primary Examiner, Art Unit 2436